

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US04/36590

A. CLASSIFICATION OF SUBJECT MATTER IPC(7) : H04L 9/00; G06F 3/00, 1/02; US CL : 380/44; 708/7, 135, 250; According to <u>International Patent Classification (IPC)</u> or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) U.S. : 380/44; 708/3, 7, 8, 100, 103, 135, 250, 491, 532		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched INSPEC search terms: modular multiplication, Barrett		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) GOOGLE search terms: Barrett, modular multiplication, random number generator		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Dham, Jean-Francois. Design of an Efficient Public-Key Cryptographic Library for RISC-based Smart Cards. Doctorate of Applied Sciences Thesis. Universite Catholique de Louvain. May 1998. Pages 11-22.	1-13
A	Barrett, Paul. Implementing the Rivest, Shamir, and Adleman Public Key Encryption Algorithm On a Standard Digital Signal Processor. Security Bulletin. Computer Security Ltd. August 1986.	1-13
A	Menezes, Oorschot, and Vanstone. Handbook of Applied Cryptography. 1997. Pages 591-635.	1-13
A	US 5,210,710 A (Omura) 11 May 1993 (11.05.1993).	1-13
A	Fu-Chi Chang, Chia-Hu Wang. Architectural tradeoff in implementing RSA processors. ACM SIGARCH Computer Architecture News archive. Volume 30, Issue 1. March 2002.	1-13
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents:		
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention	
"B" earlier application or patent published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone	
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art	
"O" document referring to an oral disclosure, use, exhibition or other means	"Z" document member of the same patent family	
"P" document published prior to the international filing date but later than the priority date claimed		
Date of the actual completion of the international search 17 March 2005 (17.03.2005)		Date of mailing of the international search report 19 APR 2005
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230		Authorized officer <i>Michelle L. Ben</i> Andrew Caldwell Telephone No. 703-305-3900